U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: ArcGIS Online
Bureau/Office: Office of the Secretary
Date: April 7, 2020
Point of Contact
Name: Teri Barnett
Title: Departmental Privacy Officer
Email: DOI_Privacy@ios.doi.gov
Phone: (202) 208-1605
Address: 1849 C Street NW, Room 7112, Washington, DC 20240

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on
- ☐ Members of the general public
- ☐ Federal personnel and/or Federal contractors
- ☐ Volunteers
- ☒ All

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

The Department of the Interior (DOI) ArcGIS Online is a cloud-based mapping and analysis solution that enables registered users including DOI employees, partners, collaborators and

members of the public to collaborate using interactive maps. Analysis tools are only available to DOI registered users though content settings may be set so site visitors and members of the public can see and use publicly available geospatial data and resources. ArcGIS Online does not maintain or display personally identifiable information (PII) beyond the limited data described in this privacy impact assessment: for the creation and management of user accounts, to allow registered users to access the analysis tools and user created content, and to monitor online content and ensure security and compliance with legal and policy requirements for use of the tool.

ArcGIS Online is a FedRAMP tailored Low-Impact - Software as a Service (LI-SaaS) provided by Esri, a geospatial cloud service provider. ArcGIS Online is a paid subscription service available to DOI bureaus and offices under the DOI-wide Enterprise License Agreement (ELA) with Esri. ArcGIS Online is centrally managed by the Geospatial Information Office within the DOI Office of the Chief Information Officer. Each DOI bureau and office that maintains an ArcGIS Online organization account designates system administrators to oversee and manage their own ArcGIS Online site content and engage with bureau personnel, partners and collaborators on projects. DOI bureaus and offices that have an ArcGIS Online account include the National Park Service, Bureau of Land Management, U.S. Fish and Wildlife Service, U.S. Geological Survey, Bureau of Reclamation, Bureau of Indian Affairs, Office of Surface Mining Reclamation and Enforcement, Bureau of Ocean Energy Management, Bureau of Safety and Environmental Enforcement, and Office of Natural Resources Revenue.

Bureau and office ArcGIS Online sites offer a customized view of ArcGIS Online and are called organizational accounts. Bureau and office ArcGIS Online organizational accounts offer flexibility to meet specific bureau and office mission objectives. These bureau and office organizational accounts are for approved organizational members only and requires each member to have an account as a registered user prior to accessing the specific bureau or office ArcGIS Online system. However, members of the public can see publicly available geospatial data and resources without becoming an organization member or creating an account. DOI ArcGIS Online organizational accounts provide approved users with an online tool to create, publish, save their work, visualize, share, search and discover geospatial data and content. Additionally, approved users can participate in topic-specific groups and collaborate on various projects using interactive maps and web applications.

DOI ArcGIS Online organization system administrators set up and configure the organizational accounts to meet their bureau or office requirements. Tools and settings are available to the administrator within the organizational account to manage user accounts, maintain security and access controls, and specify terms of use for data. The ArcGIS Online organizational account may or may not allow anonymous access to their site. If anonymous access is enabled, users can access any resources that the ArcGIS Online organization has approved for sharing with the general public without the need for a user account or signing in.

Authorized users can access their ArcGIS Online organizational account through web browsers, mobile devices and other ArcGIS components such as ArcGIS Desktop, ArcGIS Pro and ArcGIS Apps. These are license based products. Bureaus and offices have the option to utilize these

software tools that are available as part of the Esri ELA and they are each responsible for managing the appropriate use of the tools. These tools do not collect or use PII beyond the user profiles covered in this PIA. Any bureau or office that uses these additional software licenses must do so within the scope of this PIA and DOI policy. Bureaus and offices with ArcGIS Online accounts may be required to conduct a separate assessment of privacy implications for any expanded uses of PII data or technology not covered in this PIA such as development or use of a mobile application.

C. What is the legal authority?

Executive Order 12906, Coordinating Geographic Data Acquisition and Access: The National Spatial Data Infrastructure, amended by Executive Order 13286, Amendment of Executive Orders, and Other Actions, in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security; Executive Order 12951, Release of Imagery Acquired by Space-Based National Intelligence Reconnaissance Systems; OMB Circular A-16, Coordination of Geographic Information and Related Spatial Data Activities; OMB Circular A-130, Managing Information as a Strategic Resource; OMB Circular A-119, Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities; 6 U.S.C. 1523 (b)(1); E-Government Act of 2002, 44 U.S.C. 3501; and the Federal Information Security Modernization Act (FISMA) of 2014.

D. Why is this PIA being completed or modified?

☒ New Information System
☐ New Electronic Collection
☐ Existing Information System under Periodic Review
☐ Merging of Systems
☐ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☐ Other: *Describe*

E. Is this information system registered in CSAM?

☒ Yes: *Enter the UII Code and the System Security Plan (SSP) Name*

010-999993100, ArcGIS Online System Security and Privacy Plan.

☐ No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	Purpose	Contains PII *(Yes/No)*	Describe *If Yes, provide a description.*
None	None	No	N/A

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

☐ Yes: *List Privacy Act SORN Identifier(s)*
☒ No

H. Does this information system or electronic collection require an OMB Control Number?

☐ Yes: *Describe*
☒ No

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

☒ Name
☒ Personal Email Address
☒ Other: *Specify the PII collected.*

The majority of registered users are DOI employees who use official contact or work related information to create their profiles. DOI employees use their government issued Personal Identity Verification (PIV) card authenticated through the Enterprise Active Directory (AD) or a username and password issued by the bureau/office system administrator for the ArcGIS Online organization to log in to ArcGIS Online. The system collects and maintains the employee's name, official email address, username, date of last login, and role or access level for authorized users.

There is a small number of non-DOI external registered users who are partners and collaborators from other Federal, state or local agencies, academia, organizations or members of the public who use official contact or work related information to create profiles and collaborate. These individuals may voluntarily request a user account by contacting a DOI system administrator. PII required to create a user account includes the individual's name, email address, assigned role, username and password. In some cases users may voluntarily add biography information as free form text in their account profile that may include organization, contact information, areas of expertise and interests.

B. What is the source for the PII collected? Indicate all that apply.

☒ Individual
☐ Federal agency
☐ Tribal agency
☐ Local agency
☒ DOI records
☐ Third party source
☐ State agency
☒ Other: *Describe*

DOI employees (government and contractor) access ArcGIS Online by signing in with their AD credentials/DOI PIV card. Non-DOI users may request a user account by providing name and email address to system administrators to establish username and password to access ArcGIS Online. ArcGIS Online does not maintain PII beyond user account information used to authenticate users and manage access to ArcGIS Online tools.

C. How will the information be collected? Indicate all that apply.

☐ Paper Format
☒ Email
☐ Face-to-Face Contact
☒ Web site
☐ Fax
☐ Telephone Interview
☒ Information Shared Between Systems *Describe*
☒ Other: *Describe*

DOI uses AD to authenticate DOI employee users accessing ArcGIS Online. Non-DOI users may contact system administrators through the site or by email to request a new user account or update an existing account.

D. What is the intended use of the PII collected?

ArcGIS Online is not intended to maintain PII beyond user account information to provide login capability. The only PII authorized for maintenance in the system is the minimum necessary to provide login capabilities to authenticate registered users and manage access to ArcGIS Online for security purposes. User accounts are necessary in order to provide access to analysis tools, web maps, geospatial data and content, and to create and save interactive maps and applications. The use of PII is limited to the creation and management of user accounts to authenticate users, to allow authorized users to access the ArcGIS Online analysis tools and user created content, and to monitor online content and ensure security and compliance with legal and policy requirements for use of the tool. Use of the PII provides assurance of the user's identity as a

security measure. System administrators may create user groups or collaboration groups and add members to groups to share maps, create content and collaborate on projects. Registered users with certain roles may also create groups to share maps or collaborate on projects.

For policy violations such as PII included in site content, the system administrator may contact the user who is the content owner to remove the content or disable the account. For incidents, potential threats or security violations the system administrator may disable accounts and refer events to internal or external organizations as required by law and DOI policy.

E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.

☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*

User account profile information (name, username, and user provided biography in a free form text) is visible to registered users for the purpose of adding users to topic specific groups in ArcGIS Online. Name, username and user email address is visible to ArcGIS Online system administrators to manage user accounts and access to the site. System administrators also conduct reviews of user content to ensure that the information uploaded and shared within ArcGIS Online and the general public does not contain PII or sensitive information. Users may set permissions for their profiles to be viewed by the public, organization or kept private.

By default, all user-created content in ArcGIS Online is private and only accessible to the content creator and the ArcGIS Online system administrator. The user's ability to access and work with content in different ways depends on the user's role in ArcGIS Online.

☒ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*

User account profile information (name, username, and user provided biography in a free form text) is visible to registered users and ArcGIS Online system administrators. By default, all user-created and published content in ArcGIS Online is private and only accessible by the user and the ArcGIS Online system administrator. The system administrator has access to view user content to ensure data and maps created, uploaded and shared does not contain sensitive PII. Users may set permissions for their profiles to be viewed by the public, organization or kept private.

☒ Other Federal Agencies: *Describe the federal agency and how the data will be used.*

Maps and content may be shared with other Federal agencies. Other Federal agency employees may be collaborators with authorized access to AGOL. These collaborators would have the same level of access to user content as other non-DOI users. User information related to security monitoring, violations or potential threats may be shared with Federal agencies as required by law.

☒ Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

User account profile information (name, username, and biography) is visible to registered users for the purpose of adding users to topic specific groups in ArcGIS Online. In addition to name and username, user email address is visible to ArcGIS Online system administrators to manage user access and review user-created content to ensure that the information uploaded and shared within ArcGIS Online and with the general public do not contain PII or sensitive information. Users may set permissions for their profiles to be viewed by the public, organization or kept private.

By default, all user-created content in ArcGIS Online is private and only accessible to the content creator and the ArcGIS Online system administrator. The user's ability to access and work with content in different ways depends on the user's role in ArcGIS Online.

☒ Contractor: *Describe the contractor and how the data will be used.*

User account profile information may be shared with DOI contractors to communicate with users and support the system, geospatial program, and ArcGIS Online sites.

☒ Other Third Party Sources: *Describe the third party source and how the data will be used.*

By default, all user-created content in ArcGIS Online is private and only accessible to the content creator and the ArcGIS Online system administrator. The user's ability to access and work with content in different ways depends on the user's role in ArcGIS Online. User profile information (name, username, and biography) is visible to internal and external registered users in ArcGIS Online for the purpose of adding users to topic specific groups and to promote collaboration.

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

☒ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

Employees can choose not to contact the ArcGIS Online system administrator to request an account or by not accepting the ArcGIS Online system administrator's invitation to join by creating an account.

Users can stop the registration process at any time prior to submitting their information to create an account. DOI's ArcGIS Online organizational accounts use Enterprise or DOI AD and DOI Personal Identity Verification (PIV) card for authentication. Employees can choose not to sign-in using the Enterprise sign-option as a first-time user, however all ArcGIS Online users must be

identified in order to gain access to view all content shared within each ArcGIS Online organization.

- Stopping the registration process at any time prior to submitting their information to create an account
- Not signing in using the Enterprise sign-option as a first-time user
- Users also have the option to browse the ArcGIS Online organization (publicly shared content only) anonymously if the organization allows anonymous access

☐ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☐ Privacy Act Statement: *Describe each applicable format.*

☒ Privacy Notice: *Describe each applicable format.*

A Privacy Notice must be posted on the sign in page for each ArcGIS Online site.

Individuals are provided notice through the publication of this privacy impact assessment. Individuals can also view Esri's Privacy Policy located at https://www.esri.com/en-us/privacy/privacy-statements/privacy-supplement.

☒ Other: *Describe each applicable format.*

Users are presented with a DOI security warning banner on each bureau and office ArcGIS Online site that informs them they are accessing a DOI system, that they are subject to being monitored, and there is no expectation of privacy during use of the system.

☐ None

H. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

Bureau and office system administrators may retrieve the user's name, username, and email address through the ArcGIS Online administrative dashboard to review and manage user access.

I. Will reports be produced on individuals?

☒ Yes: *What will be the use of these reports? Who will have access to them?*

ArcGIS Online system administrators are the only authorized users that can use the administrative dashboard to view interactive status reports for their ArcGIS Online organization. The interactive status reports provide details on the ArcGIS Online organization's credit usage, content types created and modified, member contribution or collaboration activities, apps used, group collaborations by members, or other specific reasons such as items with insufficient metadata. Reports include username and email address of the registered user or content owner. The DOI ArcGIS Online paid subscription under the DOI-wide ELA with Esri includes credits for use by bureau and office ArcGIS Online organizational account members. Credits are the currency for specific functions when using ArcGIS Online, such as spatial analysis, routing or geocoding. Credits provide a rough measure of user and organizational use of analysis tools and are used by authorized users to run processes for projects. Only DOI system administrators may view credit usage by users, however, credit usage is not limited or monitored.

☐ No

Section 3. Attributes of System Data

A. How will data collected from sources other than DOI records be verified for accuracy?

Data provided by external users including name, username, email address are not checked for accuracy as it is presumed to be accurate at the time of submission by the user. This data is provided directly by external users who are responsible for ensuring the accuracy of the data they provide to the ArcGIS Online system administrators for account set-up and content posted in the system. DOI AD is used to verify accuracy of login credentials to authenticate DOI employees for access to ArcGIS Online.

B. How will data be checked for completeness?

Data is checked for completeness during the account creation process. Users are responsible for ensuring the completeness of the data associated with their user accounts and content posted in the system. PII data including username, email address provided by external users must be complete in order for system administrators to create accounts. ArcGIS Online relies on DOI AD to authenticate DOI employees in the system.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

User account information is provided directly by the user during account creation and can be updated by the user or by an ArcGIS Online system administrator upon request. Users are responsible for the accuracy of their records. The currency and quality of the datasets published in ArcGIS Online are the responsibility of the content owner/creator. Users can contact the ArcGIS Online organization system administrator through email on the contact information page.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

Original geospatial data is unscheduled and regarded as permanent records.

ArcGIS Online system usage records are covered under (DRS) 1.4A, Short Term Information Technology Records, System Maintenance and Use Records (DAA-0048-2013-000013), approved by the National Archives and Records Administration (NARA). These records include system operations reports, login and password files, audit trail records and backup files. The disposition is temporary. Records are cut off when superseded or obsolete and destroyed no later than 3 years after cut-off.

Records maintained in ArcGIS Online that belong to content creators are retained as long as they are active and are disposed of in accordance with applicable agency records retention schedules approved by NARA.

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

System administrators dispose of DOI records by shredding or pulping for paper records, and degaussing or erasing for electronic records in accordance with NARA Guidelines and 384 Departmental Manual 1.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

There is a limited privacy risk to internal DOI employees who are granted access to ArcGIS Online and are authenticated through the Enterprise AD. There is an increased privacy risk for external users due to the PII collected by system administrators to create and manage user accounts and authenticate users for access to ArcGIS Online. This risk is mitigated by a combination of technical, physical and administrative controls.

There is a risk that data may be inappropriately accessed or used for unauthorized purposes. In an effort to protect the privacy of individuals, DOI collects only the minimal amount of user information to create and manage user accounts and authenticate users. DOI ArcGIS Online users must be invited or added to the organization by a system administrator or authenticated using their DOI AD credentials. ArcGIS Online user accounts are properly managed, user access is authenticated and authorized, and access is restricted to authorized personnel. Additionally, elevated roles/privileges are assigned to approved users. Audit logs are used to track system activity. Inactive user accounts are disabled by system administrators based on agency defined requirements. Users are also advised not to share or publish sensitive data and the system administrators periodically review user content to ensure compliance with DOI security and privacy policies.

Firewalls and network security configurations are also built into the architecture of the system and NIST SP 800-53, Security and Privacy Controls for Federal Information Systems, and other DOI policies are fully implemented to prevent unauthorized monitoring. The DOI ArcGIS Online organization system administrators will review the use of ArcGIS Online and the activities of users to ensure that the system is not improperly used and to prevent unauthorized use or access. The DOI ArcGIS Online organization system administrator assigns roles based on the principles of least privilege and performs due diligence toward ensuring that separation of duties is in place.

All DOI employees and contractors are required to complete privacy, security and records management awareness training, as well as role-based training on an annual basis and sign the DOI Rules of Behavior prior to accessing any system to include ArcGIS Online. Security role-based training is also required for security personnel and officials with special roles and privileges. ArcGIS Online users are advised not to share sensitive data to ArcGIS Online and the system administrators review user content to ensure compliance with DOI security and privacy policies and will advise users to remove sensitive data, disable accounts, and report security or privacy violations.

There is a risk that data may be stored for longer than necessary. Records are maintained and disposed of under a NARA approved records schedule. User accounts containing PII that are inactive are disabled by system administrators, however, user created content is maintained as long as it remains active. Information collected and stored within the ArcGIS Online is maintained, protected, and destroyed in compliance with all applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. Geospatial data and maps in ArcGIS Online do not contain PII so there is no privacy risk for retention of these records.

There is potential risk to individuals due to the collection, usage, storage and sharing of geographic data and interactive mapping tools with functionalities such as (Zoom In/Out, Pan, spatial patterns, and images) in ArcGIS Online. This risk is mitigated by the system administrator reviewing user content on a regular basis and by assigning least-privilege. Users are reminded and must acknowledge a security warning banner when accessing the system.

There is a risk that PII data is collected and stored on a cloud system. Only minimal PII data is collected and used for user registration, account management and authentication purposes. ArcGIS Online is a Li-SaaS (Low impact - Software as a Service) FedRAMP authorized system and has met DOI's information security, privacy and records requirements. ArcGIS Online uses HTTPS to ensure communications are encrypted and secure to prevent information from being read, intercepted or changed during transit. User passwords are masked when signing in to ArcGIS Online sites.

There is a risk that individuals may not receive adequate notice of DOI privacy practices or the extent of the use of their PII data in ArcGIS Online. Individuals voluntarily provide their identifying information when requesting a user account to access ArcGIS Online and are provided a DOI Privacy Notice on the sign in page on the ArcGIS Online site. General notice is

provided through the publication of this privacy impact assessment. Users may also view the Privacy Statement Supplement by Esri that addresses their use, storage, sharing and disclosure of personal data collected through the use of ArcGIS Online organization accounts. Users may also contact DOI, bureau and office privacy officials with any questions or privacy concerns at https://www.doi.gov/privacy/contacts.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒ Yes: *Explanation*

The ArcGIS Online system aggregates geospatial data and makes it available to its users, which helps agencies meet their mission needs, including communicating with and publishing approved data and maps for public use.

Only minimal user information is collected to allow system administrators to manage accounts and provision users to groups and grant access to tools.

☐ No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒ No

C. Will the new data be placed in the individual's record?

☐ Yes: *Explanation*
☒ No

D. Can the system make determinations about individuals that would not be possible without the new data?

☐ Yes: *Explanation*
☒ No

E. How will the new data be verified for relevance and accuracy?

Not applicable. ArcGIS Online does not derive new data or create previously unavailable data about an individual through data aggregation.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒ No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

☒ Users
☒ Contractors
☐ Developers
☒ System Administrator
☒ Other: *Describe*

Registered users have access to publicly available and shared geospatial content as well as content shared within the organization. Users can only modify their own user-created content and update their profile information.

System administrators are the ArcGIS Online organization administrators. The system administrator controls and administers the users online services account, accesses and protects the user's data to include communication and file contents. System administrators are the only users that are authorized to make changes to user accounts. Elevated roles/privileges are granted once the request has been reviewed and approved by the administrator.

Contractors supporting DOI with a registered account have the same privileges as a user account. If a contractor is required to have an elevated role as part of an agreement with DOI, then the contractor will be granted an elevated role to satisfy the requirements of the agreement.

Anonymous users, i.e. unregistered, have access to publicly available information.

H. How is user access to data determined? Will users have access to all data or will access be restricted?

Content settings may be set so site visitors and members of the public (anonymous users) as well as registered users can see and use publicly available online geospatial data and resources.

Access as a registered user is granted by system administrators when requested by the user. Registered users are allowed to create, edit and delete their own content. Only ArcGIS Online

system administrators have access to all data within the system for the purpose of managing and administering user accounts and content.

Analysis tools are only available to DOI employees and account holders. The use of PII is limited to the creation and management of user accounts to allow authorized users to access the analysis tools and user created content, and to monitor online content and ensure security and compliance with legal and policy requirements for use of the system.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

☒ Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

Privacy Act clauses are included in the contract.

☐ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

☐ Yes. *Explanation*
☒ No

K. Will this system provide the capability to identify, locate and monitor individuals?

☒ Yes. *Explanation*

The purpose of AGOL is not to monitor individuals, however user actions and use of the system are monitored to meet DOI security policies. Data captured include username, user's last date of login, date of user content creation, date user content was modified, and credits used.

☐ No

L. What kinds of information are collected as a function of the monitoring of individuals?

Audit events in relation to the following user activities are logged: username, user's last date of login, date of user content creation, date user content was modified, credits used, and account management events.

M. What controls will be used to prevent unauthorized monitoring?

The ArcGIS Online system is not intended to monitor individuals; however, the system will have the functionality to audit the usage activity. Firewalls and network security configurations are

also built into the architecture of the system and NIST SP 800-53, Security and Privacy Controls for Federal Information Systems, and other DOI policies are fully implemented to prevent unauthorized monitoring. The DOI ArcGIS Online organization system administrator assigns roles based on the principles of least privilege and performs due diligence toward ensuring that separation of duties is in place. DOI ArcGIS Online organization system administrators review the use of ArcGIS Online and the activities of users to ensure that the system is not improperly used and to prevent unauthorized use or access. System administrators will advise users to remove sensitive data, disable accounts, and report security or privacy violations in compliance with DOI security and privacy policies.

Federal employees and Contractors must complete Federal Information System Security Awareness (FISSA) training, Privacy Awareness Training, Records Management before being granted access to the DOI network or any DOI system, and annually thereafter. In addition, some organizations implement Rules of Behavior for ArcGIS Online users for different roles or levels.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☒ Security Guards
☐ Key Guards
☒ Locked File Cabinets
☒ Secured Facility
☒ Closed Circuit Television
☐ Cipher Locks
☒ Identification Badges
☒ Safes
☐ Combination Locks
☒ Locked Offices
☒ Other. *Describe*

Badged Access Control

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☐ Biometrics
☒ Intrusion Detection System (IDS)

☒ Virtual Private Network (VPN)
☒ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☐ Other. *Describe*

(3) Administrative Controls. Indicate all that apply.

☒ Periodic Security Audits
☒ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training
☒ Regular Monitoring of Users' Security Practices
☒ Methods to Ensure Only Authorized Personnel Have Access to PII
☒ Encryption of Backups Containing Sensitive Data
☒ Mandatory Security, Privacy and Records Management Training
☐ Other. *Describe*

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The Enterprise Geospatial Information Systems (GIS) Data Manager, Office of the Chief Information Officer (OCIO) serves as the ArcGIS Online Information System Owner and the official responsible for oversight and management of the ArcGIS Online security controls and the protection of information processed and stored by the ArcGIS Online organization. The Information System Owner and Information System Security Officer are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies. Bureau and Office ArcGIS Online organization system administrators are responsible for overseeing and managing their respective organization's ArcGIS Online site and ensuring the appropriate and secure use of the system and user data.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The DOI ArcGIS Online Information System Owner and Information System Security Officer are responsible for the central oversight and management of the DOI ArcGIS Online security and privacy controls, and for ensuring to the greatest possible extent that DOI's ArcGIS Online organizational accounts are properly managed and that access is granted in a secure and auditable manner. Bureau and Office ArcGIS Online organization system administrators are also responsible for assuring proper use of the system and user data maintained for their organization's ArcGIS Online sites. The Information System Owner, Information System Security Officer and bureau and office system administrators are responsible for ensuring that

any loss, compromise, unauthorized access or disclosure of data is reported to DOI-CIRC within 1-hour of discovery in accordance with Federal policy and established DOI procedures.